(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11234647 A**

(43) Date of publication of application: **27 . 08 . 99**

(51) Int. Cl **H04N 7/167**
H04N 5/44
H04N 5/76

(21) Application number: **10032466**

(22) Date of filing: **16 . 02 . 98**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

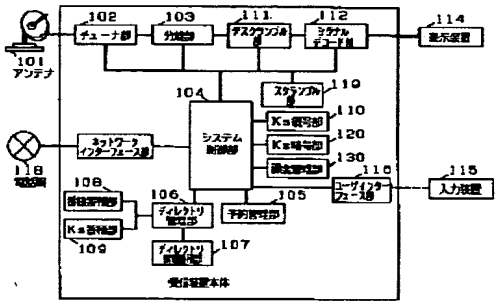
(72) Inventor: **MASUDA ISAO**
GOTO YOSHIMASA
HARADA TAKENOSUKE
MACHIDA KAZUHIRO
KATAOKA MITSUTERU
NAKAMURA YASUHIRO

(54) **STORAGE TYPE BROADCAST RECEIVER**

(57) Abstract:

PROBLEM TO BE SOLVED: To ensure the security and the copyright or the like of a stored program by encrypting the program and storing the encrypted program in the storage type receiver for a broadcast system where a broadcast program is encrypted and the encrypted program is broadcast.

SOLUTION: A Ks storage section 109 and a program storage section 108 store a scramble key that is broadcast, separated and encrypted by a separate section 103, and a program encrypted by the scramble key. When viewing the stored program, a Ks decoding section 110 decodes the scramble key. A descramble section 111 descrambles the encrypted program by using a decoded scramble key and the decoded program is viewed on a display device 114. The security of the stored program is protected by storing the encrypted program in this way.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－234647

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ	7/167	Ｈ０４Ｎ	7/167	Ｚ
	5/44		5/44	Ａ
	5/76		5/76	Ｚ

審査請求　未請求　請求項の数14　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－32466

(22)出願日　平成10年(1998)２月16日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　増田　功
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　後藤　吉正
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　原田　武之助
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外１名）

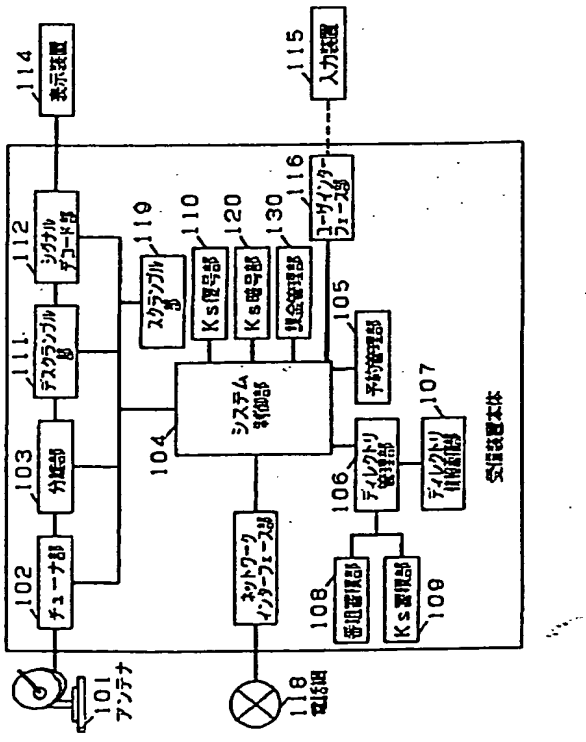
最終頁に続く

(54)【発明の名称】　蓄積型放送受信装置

(57)【要約】

【課題】　放送番組を暗号化して放送する放送システムの蓄積型の受信装置において、番組を暗号化して蓄積することによって、蓄積された番組の秘匿性や著作権などを保持することを目的とする。

【解決手段】　放送され、分離部１０３によって分離された暗号化したスクランブル鍵とそのスクランブル鍵によって暗号化した番組を、Ｋｓ蓄積部１０９、および番組蓄積部１０８に蓄積する。蓄積した番組を視聴する際にスクランブル鍵をＫｓ復号部１１０において復号する。デスクランブル部１１１において、復号化したスクランブル鍵を使って、暗号化した番組を復号化し、表示装置１１４において視聴する。このように番組を暗号化して蓄積することによって、蓄積された番組の秘匿性を保護することが出来る。



【特許請求の範囲】

【請求項１】　スクランブル鍵を用いて放送番組を暗号化し、放送番組の秘匿性を保持する放送システムの放送受信装置であって、前記スクランブル鍵を蓄積するスクランブル鍵蓄積部と、前記スクランブル鍵によって暗号化された前記放送番組を蓄積する番組蓄積部を有したことを特徴とする蓄積型放送受信装置。

【請求項２】　前記スクランブル鍵によって暗号化された放送番組を番組蓄積部へ蓄積する時に課金することを特徴とする請求項１記載の蓄積型放送受信装置。

【請求項３】　前記番組蓄積部に蓄積されている放送番組を番組蓄積部から表示する時に課金することを特徴とする請求項１記載の蓄積型放送受信装置。

【請求項４】　前記放送システムからのスクランブル鍵の変更要求に基づき、スクランブル鍵蓄積部に蓄積されているスクランブル鍵を変更するスクランブル鍵更新手段を有することを特徴とする請求項１記載の蓄積型放送受信装置。

【請求項５】　前記スクランブル鍵更新手段は、放送システムからのスクランブル鍵の更新要求に基づき、スクランブル鍵蓄積部に蓄積されているスクランブル鍵を更新する前に、スクランブル鍵によって暗号化され前記番組蓄積部に蓄積されている放送番組を復号化することを特徴とする請求項４記載の蓄積型放送受信装置。

【請求項６】　前記スクランブル鍵更新手段は、放送システムからのスクランブル鍵の更新要求に基づき、新しいスクランブル鍵をスクランブル鍵蓄積部に追加蓄積することにより、スクランブル鍵蓄積部に複数のスクランブル鍵を蓄積することを可能にした請求項４記載の蓄積型放送受信装置。

【請求項７】　前記スクランブル鍵更新手段は、放送システムからのスクランブル鍵の変更要求に基づき、スクランブル鍵蓄積部に蓄積されているスクランブル鍵を更新する前に、スクランブル鍵を用いて暗号化され番組蓄積部に蓄積されている放送番組を復号化し、新しいスクランブル鍵を用いて再度暗号化することを特徴とする請求項４記載の蓄積型放送受信装置。

【請求項８】　前記番組蓄積部の暗号化された蓄積番組を検索し、蓄積した放送番組の番組一覧を作成することを特徴とする請求項１または請求項４記載の蓄積型放送受信装置。

【請求項９】　放送番組を蓄積する番組蓄積部と、この番組蓄積部に蓄積されている前記放送番組をディレクトリ情報によって管理するディレクトリ管理部と、このディレクトリ管理部において生成される前記番組蓄積部に蓄積されている前記放送番組を管理する情報であるディレクトリ情報を前記放送システムによって放送されたディレクトリスクランブル鍵によって暗号化するディレクトリ情報暗号部と、前記ディレクトリスクランブル鍵を蓄積するディレクトリスクランブル鍵蓄積部を有した蓄積型放送受信装置。

【請求項１０】　放送システムからのディレクトリスクランブル鍵の変更要求に基づき、ディレクトリスクランブル鍵蓄積部に蓄積されているディレクトリスクランブル鍵を変更するディレクトリスクランブル鍵更新手段を有することを特徴とする請求項９記載の蓄積型放送受信装置。

【請求項１１】　前記ディレクトリスクランブル鍵更新手段は、放送システムからのディレクトリスクランブル鍵の更新要求に基づき、ディレクトリスクランブル鍵蓄積部に蓄積されているディレクトリスクランブル鍵を更新する前に、ディレクトリスクランブル鍵によって暗号化され上記ディレクトリ情報蓄積部に蓄積されているディレクトリ情報を復号化することを特徴とする請求項１０記載の蓄積型放送受信装置。

【請求項１２】　ディレクトリスクランブル鍵更新手段は、放送システムからのディレクトリスクランブル鍵の更新要求に基づき、新しいディレクトリスクランブル鍵を前記ディレクトリスクランブル鍵蓄積部に追加蓄積することにより、ディレクトリスクランブル鍵蓄積部に複数のディレクトリスクランブル鍵を蓄積可能にした請求項１０記載の蓄積型放送受信装置。

【請求項１３】　前記ディレクトリスクランブル鍵更新手段は、放送システムからのディレクトリスクランブル鍵の変更要求に基づき、ディレクトリスクランブル鍵蓄積部に蓄積されているディレクトリスクランブル鍵を更新する前に、該ディレクトリスクランブル鍵を用いて暗号化されディレクトリ情報蓄積部に蓄積されているディレクトリ情報を復号化し、新しいディレクトリスクランブル鍵を用いて再度暗号化することを特徴とする請求項１０記載の蓄積型放送受信装置。

【請求項１４】　前記番組蓄積部の蓄積番組を、暗号化されたディレクトリ情報から検索し、蓄積した放送番組の番組一覧を作成することを特徴とする請求項９または請求項１０記載の蓄積型放送受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル放送システムにおいて蓄積装置を備え、蓄積された番組に対してアクセス制御、課金を行なうことができる蓄積型放送受信装置に関するものである。

【０００２】

【従来の技術】近年、通信技術およびデータ処理技術の発展によりオーディオ情報やビジュアル情報といったマルチメディア情報がディジタル化されて利用者に提供されるようになり、また大容量の記憶媒体の登場により大量のデータを放送し、ユーザ側の端末装置で受信、蓄積し、任意のタイミングで視聴するという放送システムが可能な状況になってきている。また、限定された視聴者のみに番組を視聴可能にする限定受信システムが、衛星

ディジタル放送において、サービスが可能になっている。図２１に、現在実用化されている衛星ディジタル放送である、ＰｅｒｆｅｃＴＶの限定受信システムの構成を示す。１１は、映像などの番組データである。１２は、映像などの番組データをスクランブルするためのスクランブル鍵である。１３は、スクランブル鍵を暗号化するワーク鍵である。１４は、送信側においてワーク鍵を暗号化するマスタ鍵である。１５は、受信側においてワーク鍵を復号化するマスタ鍵である。まず番組データ１１を、スクランブル鍵１２によって、スクランブルする（Ｓ（ステップ）１６）。そのスクランブル鍵１２を、ワーク鍵１３によって暗号化する（Ｓ１７）。そのワーク鍵１３を、マスタ鍵１４によって暗号化する（Ｓ１８）。暗号化されたスクランブル鍵、暗号化されたワーク鍵を、スクランブルされた番組のデータと多重する（Ｓ１９）。多重したデータを衛星波によって放送する（Ｓ２０）。多重データを受信し、受信装置において、スクランブルされた番組のデータ、暗号化されたスクランブル鍵、暗号化されたワーク鍵を分離する（Ｓ２１）。暗号化されたワーク鍵を、マスタ鍵１５によって復号化する（Ｓ２２）。暗号化されたスクランブル鍵を、復号化されたワーク鍵によって復号化する（Ｓ２３）。復号化されたスクランブル鍵を使って、スクランブルされた番組データをデスクランブルする（Ｓ２４）。デスクランブルされた番組のデータを表示装置に送り、表示する（Ｓ２５）。

【０００３】番組の蓄積に関しては、特開昭６３－１０７２８１号公報に開示した番組コピー防止技術のように、再録画防止を目的としたものがある。

【０００４】

【発明が解決しようとする課題】しかしながら、従来における番組コピー防止技術は、再録画防止を目的としたものであるので、番組をスクランブルしたまま、蓄積することができない。また、ＰｅｒｆｅｃＴＶのシステムにおいては、番組を受信した時点で課金が行われていた。番組をスクランブルしたまま蓄積し、視聴するときにデスクランブルする手段を持たなかった。そのため、番組の秘匿性を保ったまま、視聴者が蓄積された番組を見た場合のみに課金することが出来なかった。また、蓄積された番組のアクセス制御を行なうために用いられる暗号鍵を更新する手段を持たなかった。そのため、その暗号化鍵を破られた場合に、蓄積番組を保護するために、鍵の更新を行なう方法を持たなかった。

【０００５】

【課題を解決するための手段】この課題を解決するために、本発明は、第１に、スクランブルした番組を蓄積し、それを管理する情報を蓄積する手段を備えるものである。これにより、番組の秘匿性を保ちながら、番組を蓄積し、蓄積した番組の視聴が可能になる。第２に、端末に番組を蓄積し、それを管理するディレクトリ情報をスクランブルして蓄積する手段を備えたものである。これにより、番組の秘匿性を保ちながら、番組を蓄積し、蓄積した番組の視聴が可能になる。

【０００６】

【発明の実施の形態】（実施の形態１）以下、本発明の実施の形態について、図を用いて説明する。

【０００７】図１は、番組を暗号化して蓄積することができる受信端末の構成図を示す。図１において、１０１は放送波を受信するアンテナである。１０２は、アンテナから受信された放送波から希望するトランスポートストリーム、ＴＳ（Ｔｒａｎｐｏｒｔ Ｓｔｒｅａｍ）を選択し受信するチューナ部である。ＴＳは、ＭＰＥＧ２システム規格に準拠したトランスポート・パケットからなる。１０３は、受信したＴＳから番組データ、番組データのスクランブルを解くスクランブル鍵、番組管理情報等を分離する分離部である。１０４は、各部から各種情報を受け取り、一定処理を行ない、他の部へ情報を送り出すシステム制御部である。１０５は、システム制御部１０４から予約に関する情報を受け取り、予約管理情報を生成し予約管理を行なう予約管理部である。１０６は、システム制御部１０４から蓄積する番組に関する情報と、番組データやスクランブル鍵を受け取り、蓄積番組を管理するディレクトリ情報を生成し、蓄積番組を管理するディレクトリ管理部である。１０７は、ディレクトリ管理部１０６からディレクトリ情報を受け取り保存するディレクトリ情報蓄積部である。１０８は、ディレクトリ管理部１０６から番組データを受け取り、指定されたアドレスに蓄積する番組蓄積部である。１０９は、スクランブル鍵を蓄積するＫｓ蓄積部である。１１０は、分離部１０３から分離されたスクランブル鍵の復号化を行うＫｓ復号部である。１１１は、分離部１０３または、システム制御部からスクランブルされた番組データを受け取り、Ｋｓ復号部からスクランブル鍵を受け取り、番組データの復号化を行なうデスクランブル部である。１１２は、デスクランブル部から番組データを受け取り、表示装置１１４に表示できる形式に信号を変換するシグナルデコード部である。１１３は、番組管理情報から課金情報を取り出し、課金情報を管理蓄積する課金管理部である。１１４は、番組や各種情報を表示する表示装置である。１１５は、ユーザの要求を受け付ける入力装置である。１１６は、入力装置１１５からの入力を受け付けるユーザインタフェースである。１１７は、システム制御部１０４から受け取った情報を外部ネットワーク、この場合電話網１１８に出力するネットワークインターフェース部である。１１８は、外部ネットワークである電話網である。１１９は、番組データの暗号化を行なうスクランブル部である。１２０は、スクランブル鍵の暗号化を行なうＫｓ暗号部である。

【０００８】図２は、スクランブル鍵が配信される時の状態であるスクランブル鍵情報３０１である。スクラン

ブル鍵情報３０１は、暗号化されたスクランブル鍵本体３０４のほかに、スクランブル鍵を特定するためのＫｓＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）３０２が割り当てられ、スクランブル鍵が配信された配信日３０３が付加されている。

【０００９】図３は、番組を管理する情報である番組管理情報４０１である。番組管理情報４０１は、番組を特定するための番組ＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）４０２と、その番組が放映されるチャンネル４０３と日時４０４、その番組に対する課金情報４０５、番組のタイトル４０８、あらすじ等の情報が記述されている番組情報４０９からなる。また、課金情報は、サブフィールドを持ち、課金種別４０６と、課金価格４０７に別れている。

【００１０】図４は、放送波によって配信されるＥＰＧ情報である番組プログラム管理情報５０１である。番組プログラム管理情報５０１は、現在放送されている、あるいは放送予定の番組管理情報４０１の一覧である。

【００１１】図５は、予約管理部１０５において、番組の蓄積の予約を管理する予約管理情報６０１である。予約管理情報６０１は、予約管理識別子である予約管理ＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）６０２と番組管理情報４０１からなる。

【００１２】図６は、ディレクトリ管理部１０６において、蓄積番組を管理するディレクトリ情報７０１である。ディレクトリ情報は、蓄積管理ＩＤ７０２と、番組データを蓄積する際の蓄積先頭アドレス７０３、蓄積サイズ７０４、番組の暗号化を行っているスクランブル鍵のＫｓ　ＩＤ７０５、番組管理情報４０１からなる。

【００１３】図７は、視聴者が番組を予約するための番組一覧画面８０１である。図の８０２が、視聴者によって選択された番組である。

【００１４】図８は、蓄積された番組を視聴者が選択できるようにするための蓄積番組一覧表画面９０１である。図の９０２が視聴者によって、選択された番組である。

【００１５】本発明の特徴である放送番組を蓄積受信する場合の一般的な蓄積予約について説明する。放送番組や、その他情報は、放送波によって多重されて放送されている。ユーザが入力装置１１５によって番組一覧の表示を要求すると、その時受信されているトランスポートストリーム、ＴＳ（Ｔｒａｎｐｏｒｔ　Ｓｔｒｅａｍ）から分離部１０３によって番組に関するＥＰＧ（Ｅｌｅｃｔｒｉｃ　Ｐｒｏｇｒａｍ　Ｇｕｉｄｅ）情報を分離する。このシステムにおけるＥＰＧ情報は、プログラム管理情報５０１である。そのプログラム管理情報５０１をシステム制御部１０４において、ユーザが番組一覧から選択できる番組一覧画面８０１に変換し、シグナルデコード部１１２を通して、表示装置１１４に表示する。ユーザは、表示された番組一覧画面８０１から、蓄積予約したい番組を入力装置１１５によって選択する。ユーザが入力装置１１５によって、蓄積予約を決定すると、システム制御部１０４は、その番組管理情報４０１を取り出し、予約管理部１０５に送る。予約管理部１０５は、予約管理情報６０１を生成する。予約管理情報６０１は、予約管理部１０５において管理保存される。番組の蓄積の動作を図９を用いて説明する。予約管理部１０５は、常に予約管理情報６０１の番組管理情報４０１中の日時情報４０４を監視している。予約管理情報６０１の番組管理情報４０１中の日時情報４０４で、蓄積時間が来た番組について、予約管理部１０５は、システム制御部１０４に対して予約管理情報６０１の番組管理情報４０１を送り出す。システム制御部１０４は、蓄積すべきチャンネルを含むＴＳを受信するようチューナ部１０２に要求する。チューナ部１０２はそのＴＳを受信する（Ａ１）。受信されたＴＳは、分離部１０３において、スクランブルをかけられた番組データとスクランブル鍵情報３０１に分離される（Ａ２）。番組データは、映像や音声のシグナルデータからなる、ＭＰＥＧ２トランスポートパケットである。このパケットには、番組に使われる映像や音声データのパケットを識別するためのパケット識別子ＰＩＤ（Ｐａｃｋｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）が割り当てられている。このＰＩＤは、番組が変わるときに、同時に変更される。新しいスクランブル鍵情報３０１を受信した時、そのスクランブル鍵情報３０１は、Ｋｓ蓄積部１０９に蓄積される。分離された番組データと番組管理情報４０１は、ディレクトリ管理部１０６へ送られる。番組データは、番組蓄積部１０８において、ディレクトリ管理部１０６が指定した蓄積先頭アドレス７０３に蓄積される（Ａ３）。番組データの終わりは、番組データに使われているデータのＰＩＤが変更されたことによって知る。番組データの終わった時点で、蓄積をやめる（Ａ４）。ディレクトリ管理部１０６は、番組管理情報４０１、蓄積されている先頭アドレス、番組データの蓄積サイズ、番組のスクランブルを行なっているスクランブル鍵のＫｓ　ＩＤから、ディレクトリ情報７０１を生成する（Ａ５）。ディレクトリ情報をディレクトリ情報蓄積部１０７に蓄積する（Ａ６）。この時、番組データはスクランブルをかけられたまま蓄積されるので、番組の秘匿性を保ったまま蓄積できる。また、ディレクトリ情報７０１は、ディレクトリ情報蓄積部１０７に保存される。蓄積された番組の視聴の一例をしめす。まず、ディレクトリ管理部１０６は、ディレクトリ情報蓄積部１０７に保存されているディレクトリ情報７０１から、必要な情報をシステム制御部１０４に送り出す。システム制御部１０４では、それら情報から、蓄積番組の一覧表画面９０１を作成する。蓄積番組一覧表画面９０１は、シグナルデコード部１１２を通して、表示装置１１４に表示される。ユーザは、その一覧から視聴したい番組を、入力装置１１５によって選択し、決定する。番組が決定されると、ディレクトリ管理部１０

６は、蓄積管理ＩＤ　７０２から、決定された番組を選択する。また、Ｋｓ　ＩＤ７０５をＫｓ蓄積部１０９へ送り出し、そのＫｓ　ＩＤ７０５を持つスクランブル鍵３０４を取り出す。そのスクランブル鍵３０４は、Ｋｓ復号部において、復号化される。また、システム制御部１０４は、選択された蓄積管理ＩＤ７０２から、蓄積先頭アドレス７０３と蓄積サイズ７０４を取り出す。番組蓄積部１０８のそのアドレスに蓄積されている番組データを取り出し、デスクランブル部へ送る。復号化されたスクランブル鍵も、デスクランブル部へ送られ、そのスクランブル鍵を使って番組データを復号化する。復号化された番組データは、シグナルデコード部１１２において、表示装置１１４に表示できる形式にデコードされ、最終的に表示装置１１４に表示される。番組蓄積部１０８から蓄積サイズ分のデータを取り出した時点で、それらの処理を終了する。

【００１６】受信装置に蓄積されている番組に対して、蓄積時に課金を行う場合の動作を説明する。

【００１７】図１０は、課金管理部１１３において管理されている課金管理情報１００１である。課金管理情報１００１は、番組ＩＤ　１００２と課金価格１００３からなる。

【００１８】番組データの蓄積時に分離部１０３から分離された番組プログラム管理情報５０１の番組管理情報４０１をディレクトリ管理部１０６に送る際、システム制御部１０４は、番組管理情報４０１の課金情報４０５中の課金種別４０６で蓄積時課金が指定されているかを確認する。蓄積時課金が指定されている場合、システム制御部１０４は、その番組ＩＤ　４０２と課金情報４０５を課金管理部１１３に送る。課金管理部１１３は、それらの情報から、番組ＩＤ１００２とその課金価格１００３を一覧にした課金管理情報１００１を生成し保存する。課金管理情報１００１は、定期的にネットワークインターフェース部１１７から電話網１１８を通じて放送局等の課金ホストシステムに送られる。

【００１９】受信装置に蓄積されている番組に対して、視聴時に課金を行う場合の動作を説明する。蓄積された番組を視聴するとき、システム制御部１０４は、ディレクトリ情報７０１から表示画面用の情報を取り出している。その時、番組管理情報４０１の課金情報４０１中の課金種別４０６の中で視聴時課金が指定されているかを確認する。視聴時課金が指定されている場合、システム制御部１０４は、その番組ＩＤ４０２と課金情報４０５を課金管理部１１３に送る。課金管理部１１３は、それらの情報から、番組ＩＤ１００２とその課金価格１００３を一覧にした課金管理情報１００１を生成し保存する。課金管理情報は、定期的にネットワークインターフェース部１１７から電話網１１８を通じて放送局等の課金ホストシステムに送られる。

【００２０】スクランブル鍵更新の動作を説明する。Ｋｓが配信されるとき、スクランブル鍵情報３０１として配信される。スクランブル鍵情報３０１は、Ｋｓ蓄積部１０９に保存される。放送システムからのスクランブル鍵更新要求は、新しいスクランブル鍵の配信によって行われる。新しいスクランブル鍵情報３０１が配信されるとき、Ｋｓ　ＩＤ　３０２が変更されている。受信端末のシステム制御部１０４では、常にＫｓ蓄積部１０９に保存されているスクランブル鍵情報３０１のＫｓＩＤ　３０２と、受信されたスクランブル鍵情報のＫｓ　ＩＤ　３０２とを比較している。Ｋｓ蓄積部１０９に保存されているＫｓ　ＩＤと異なるＫｓ　ＩＤが受信されたとき、スクランブル鍵の更新が行なわれる。

【００２１】Ｋｓ蓄積部１０９がスクランブル鍵を１つしか保存しない場合の動作の一例を、図１２を用いて示す。スクランブル鍵を更新する場合、新しいスクランブル鍵情報３０１を放送する。システム制御部（スクランブル鍵更新手段）１０４では、Ｋｓ蓄積部１０９に蓄積されているスクランブル鍵３０１のＫｓ　ＩＤ３０２と、受信されたスクランブル鍵のＫｓ　ＩＤ３０２の比較を常に行なっている。蓄積されているＫｓ　ＩＤ３０２と受信されたＫｓ　ＩＤ３０２が異なる場合、スクランブル鍵の更新を受け付ける（１２０２）。Ｋｓ蓄積部１０９に蓄積されているスクランブル鍵情報３０１を削除する（１２０３）。受信されたスクランブル鍵情報３０１を、Ｋｓ蓄積部１０９に蓄積する（１２０４）。

【００２２】さらに本発明によれば、請求項６のように、スクランブル鍵を追加蓄積する場合がある。その場合の動作の一例を、図１３を用いて示す。スクランブル鍵を更新する場合、新しいスクランブル鍵情報３０１を放送する。システム制御部（スクランブル鍵更新手段）１０４では、Ｋｓ蓄積部１０９に蓄積されているＫｓＩＤ　３０２と、受信されたスクランブル鍵情報３０１のＫｓ　ＩＤ３０２の比較を常に行なっている。受信されたスクランブル鍵のＫｓ　ＩＤ３０２が、蓄積されているスクランブル鍵のＫｓＩＤ５０２といずれも一致しなかった場合、スクランブル鍵更新を受け付ける（１３０２）。そして、Ｋｓ蓄積部１０９に空領域があるかないかを調べる（１３０３）。Ｋｓ蓄積部１０９に空領域がある場合、その空領域に受信されたスクランブル鍵情報３０１を保存する（１３０６）。Ｋｓ蓄積部１０９に空領域がない場合、配信日が最も古いスクランブル鍵情報３０１を検索しする（１３０４）。その最も古いスクランブル鍵情報３０１を削除する（１３０５）。削除された空領域に、新しく受信されたスクランブル鍵情報３０１を保存する（１３０６）。

【００２３】スクランブル鍵を更新したときに、更新前のＫｓで暗号化された蓄積番組を復号化して蓄積し、スクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合、Ｋｓ蓄積部１０９は、スクランブル鍵を１つしか保存しない。スクランブル鍵が更新

されると、システム制御部１０４は、更新前のスクランブル鍵情報３０１をＫｓ蓄積部１０９から取り出す。その中のＫｓ　ＩＤ　３０２をディレクトリ管理部１０６に送る。ディレクトリ管理部１０６の中から、更新前のＫｓ　ＩＤ３０２　とディレクトリ情報中７０１のＫｓ　ＩＤ７０５と一致するディレクトリ情報７０１を取り出す。その情報の蓄積先頭アドレス７０３から番組データを番組蓄積部１０８から取りだす。システム制御部１０４は、更新前のスクランブル鍵と番組データをデスクランブル部に送り出す。デスクランブル部は、暗号化された番組データを更新前のスクランブル鍵で復号化し、復号化された番組データを、システム制御部１０４に送り出す。システム制御部１０４は、番組データ、番組情報をディレクトリ管理部１０６に送り出す。ディレクトリ管理部１０６では、新たに蓄積管理ＩＤ７０２、蓄積先頭アドレス７０３を割り振り、Ｋｓ　ＩＤ７０５には何も指定せずに、ディレクトリ情報７０１を生成し、ディレクトリ情報蓄積部１０７に保存する。

【００２４】このように蓄積された番組を視聴する場合の一例を示す。視聴者が視聴要求したとき、そのディレクトリ情報７０１のＫｓ　ＩＤ７０５に何も指定がなかった場合、その番組データは、シグナルデコード部１１２に送られ、表示装置１１４に表示できる形式に変化された後、表示装置１１４に表示される。

【００２５】スクランブル鍵を更新したときに、更新前のＫｓを複数個蓄積し、スクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。スクランブル鍵が更新された場合、新しいスクランブル鍵情報３０１が放送される。システム制御部１０４では、Ｋｓ蓄積部１０９に蓄積されているスクランブル鍵のＫｓ　ＩＤ３０２と、受信されたスクランブル鍵のＫｓ　ＩＤ３０２の比較を常に行なっている。受信されたスクランブル鍵のＫｓ　ＩＤ３０２が、蓄積されているスクランブル鍵のＫｓ　ＩＤ３０２といずれも一致しなかった場合、Ｋｓ蓄積部１０９の空領域に、受信されたスクランブル鍵情報３０１をＫｓ蓄積部１０９に保存する。Ｋｓ蓄積部１０９に空領域がない場合、配信日の最も古いスクランブル鍵情報が取り出され、Ｋｓ蓄積部１０９内のスクランブル鍵情報が削除される。システム制御部１０４は、取り出されたスクランブル鍵情報のＫｓ　ＩＤをディレクトリ管理部１０６に送る。ディレクトリ管理部１０６は、ディレクトリ情報蓄積部１０７にあるディレクトリ情報７０１から、Ｋｓ　ＩＤと一致するディレクトリ情報を消去し、同時に、その情報の蓄積先頭アドレスに蓄積されている番組データを消去する。また、Ｋｓ蓄積部１０９のＫｓ蓄積部１０９の削除された空領域に、新しく受信されたスクランブル鍵情報３０１を保存する。

【００２６】スクランブル鍵を更新したときに、更新前のＫｓで暗号化された番組を復号化し、新しいスクランブル鍵で再暗号化して蓄積し、スクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合にも、Ｋｓ蓄積部１０９は、スクランブル鍵を1つしか保存しない。スクランブル鍵が更新された場合、システム制御部１０４は、Ｋｓ蓄積部１０９から更新前のスクランブル鍵を取り出し、Ｋｓ復号部２１０へ送る。Ｋｓ復号部で復号されたスクランブル鍵は、デスクランブル部１１１へ送られる。更新されたスクランブル鍵も、Ｋｓ復号部１１０で復号化される。復号化された新しいスクランブル鍵は、スクランブル部１１９へ送られる。また、システム制御部１０４は、スクランブル鍵が更新されたことをディレクトリ管理部１０６に伝える。ディレクトリ管理部１０６では、ディレクトリ情報蓄積部１０７に保存されているディレクトリ情報７０１を参照し、更新前のＫｓ　ＩＤを持つディレクトリ情報７０１と番組データを取り出し、システム制御部１０４へ送る。システム制御部１０４は、更新前の番組データをデスクランブル部１１１へ送り、番組データを復号化する。復号された番組データは、スクランブル部１１９へ送られ、新しいスクランブル鍵によって暗号化される。暗号化された番組データは、システム制御部１０４へ送られる。システム制御部１０４は、番組データと暗号を行なったスクランブル鍵のＫｓ　ＩＤをディレクトリ管理部１０６へ送る。ディレクトリ管理部１０６は、再スクランブルされた番組データに対して、新たにディレクトリ情報７０１を作成する。そのとき、Ｋｓ　ＩＤ７０５は、暗号化を行なった更新後のスクランブル鍵のＫｓＩＤに置き換え、新たに蓄積する蓄積先頭アドレス７０３を記述して、作成する。番組データは、番組蓄積部２０８のその蓄積先頭アドレスに蓄積される。番組データの再暗号化を行なったスクランブル鍵は、Ｋｓ暗号部１２０に送られ、暗号化される。暗号化されたスクランブル鍵は、システム制御部１０４において、新しいスクランブル鍵情報３０１を再構成され、Ｋｓ蓄積部２０９に蓄積される。ディレクトリ情報７０１から蓄積番組用の番組一覧を作成する方法の動作を説明する。

【００２７】図１１は、蓄積番組用の番組一覧を表示するためにシステム制御部１０４において生成される蓄積番組表示情報である。１１０２は、蓄積番組を特定するための蓄積管理　ＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）、１１０３は蓄積された番組のチャンネル、１１０４は蓄積された番組が放送された日時、１１０５は蓄積された番組の課金情報、１１０６はそのサブフィールドである課金種別、１１０７はその課金価格、１１０８は蓄積された番組のタイトル、１１０９は蓄積された番組の番組情報である。

【００２８】まず、ディレクトリ管理部１０６は、ディレクトリ情報蓄積部１０７に保存されている蓄積管理情報７０１から、蓄積管理ＩＤ７０２、番組管理情報４０１の中のチャンネル４０３、日時４０４、タイトル４０８、課金情報４０５、番組情報４０９を取り出し、シス

テム制御部１０４へ送る。これらの情報から、蓄積番組表示情報１１０１を生成する。蓄積番組表時情報１１０１の日時情報１１０４から、蓄積番組一覧画面８０１の日付、開始時間、終了時間を作り、蓄積番組表時情報のチャンネル１１０３から蓄積番組一覧画面のチャンネルを作り、蓄積番組表時情報のタイトル１１０８から、蓄積番組一覧画面のタイトルを生成し、図９の蓄積番組一覧画面を表示装置１１４に表示する。

【００２９】（実施の形態２）ディジタル放送における、蓄積番組の管理情報を暗号化して保存する受信端末の構成図を図１４に示す。

【００３０】図１４において、２０１は放送波を受信するアンテナである。２０２は、アンテナから受信された放送波から希望するトランスポートストリーム、ＴＳ（Ｔｒａｎｐｏｒｔ Ｓｔｒｅａｍ）を選択し受信するチューナ部である。ＴＳは、ＭＰＥＧ２システム規格に準拠したトランスポート・パケットからなる。２０３は、受信したＴＳから番組データ、スクランブル鍵、ディレクトリスクランブル鍵、番組プログラム管理情報を分離する分離部である。２０４は、各部から各種情報を受け取り、一定処理を行ない、他の部へ情報を送り出すシステム制御部である。２０５は、システム制御部２０４から予約に関する情報を受け取り、予約管理情報を生成し予約管理を行なう予約管理部である。２０６は、システム制御部２０４から蓄積する番組に関する情報と、番組データやスクランブル鍵を受け取り、蓄積番組を管理するディレクトリ情報を生成し、蓄積番組を管理するディレクトリ管理部である。２０７は、ディレクトリ管理部２０６からディレクトリ情報を受け取り保存するディレクトリ情報蓄積部である。２０８は、ディレクトリ管理部２０６から番組データを受け取り、指定されたアドレスに蓄積する番組蓄積部である。２０９は、ディレクトリ情報７０１の暗号／復号化を行なうディレクトリスクランブル鍵を蓄積するＫｄ蓄積部である。２１０は、分離部２０３から分離されたスクランブル鍵の復号化を行うＫｓ復号部である。２１１は、分離部２０３または、システム制御部からスクランブルされた番組データを受け取り、Ｋｓ復号部からスクランブル鍵を受け取り、番組データの復号化を行なうデスクランブル部である。２１２は、デスクランブル部から番組データを受け取り、表示装置２１４に表示できる形式に信号を変換するシグナルデコード部である。２１３は、番組管理情報から課金情報を取り出し、課金情報を管理蓄積する課金管理部である。２１４は、番組や各種情報を表示する表示装置である。２１５は、ユーザの要求を受け付ける入力装置である。２１６は、入力装置２１５からの入力を受け付けるユーザインタフェースである。２１７は、システム制御部２０４から受け取った情報を外部ネットワーク、この場合電話網２１８に出力するネットワークインターフェース部である。２１８は、外部ネットワークである電話網である。２１９は、番組データの暗号化を行なうスクランブル部である。２２０は、分離部２０３から分離された暗号化されたディレクトリスクランブル鍵の復号化を行なうＫｄ復号部である。２２１は、ディレクトリスクランブル鍵の暗号化を行なうＫｄ暗号部である。２２２は、ディレクトリ情報７０１をディレクトリスクランブル鍵を使って暗号を行なう、ディレクトリ情報暗号部である。２２３は、暗号化されたディレクトリ情報７０１を、ディレクトリスクランブル鍵を使って復号を行なうディレクトリ情報復号部である。

【００３１】図１５は、ディレクトリスクランブル鍵が配信される時の状態であるディレクトリスクランブル鍵情報である。ディレクトリスクランブル鍵情報１４０１は、暗号化されたディレクトリスクランブル鍵本体１４０４のほかに、ディレクトリスクランブル鍵識別子であるＫｄ ＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）１４０２と、ディレクトリスクランブル鍵が配信された配信日１４０３が付加されている。

【００３２】図１６は、ディレクトリ管理部２０６によって生成される暗号化される前のディレクトリ情報１５０１である。ディレクトリ情報１５０１は、蓄積された番組データを特定するための蓄積管理ＩＤ（Ｉｄｅｎｔｉｆｉｅｒ）１５０２、番組データを蓄積する際の蓄積先頭アドレス１５０３、番組データの合計サイズである蓄積サイズ１５０４、番組管理情報４０１からなる。

【００３３】図１７は、ディレクトリ情報蓄積部２０７に蓄積される、暗号化された後のディレクトリ情報１６０１である。暗号化ディレクトリ情報１６０１は、ディレクトリスクランブル鍵識別子Ｋｄ ＩＤ １６０２、蓄積管理ＩＤ １６０３、暗号化蓄積先頭アドレス１６０４、暗号化蓄積サイズ１６０５、番組管理情報４０１からなる。

【００３４】この場合の番組の蓄積の一例を、図１８を用いて説明する。予約管理部２０５は、常に予約管理情報６０１の番組管理情報４０１中の日時情報４０４を監視している。予約管理情報４０１の中の日時情報４０４で、蓄積時間が来た番組について、予約管理部２０５は、システム制御部２０４に対して予約管理情報６０１の番組管理情報４０１を送り出す。システム制御部２０４は、蓄積すべきチャンネルを含むＴＳを受信するようチューナ部２０２に要求する。チューナ部２０２はそのＴＳを受信する（Ｂ１）。受信されたＴＳを、分離部２０３において、スクランブルをかけられた番組データ、スクランブル鍵情報３０１、ディレクトリスクランブル鍵情報１４０１に分離する（Ｂ２）。スクランブル鍵情報を、Ｋｓ復号部２１９へ送り、スクランブル鍵を復号する（Ｂ３）。受信された、またはＫｄ蓄積部２０９に蓄積されているディレクトリスクランブル鍵情報１４０１を、Ｋｄ復号部２２０に送り復号する（Ｂ４）。復号化されたスクランブル鍵は、システム制御部２０４に戻

され、デスクランブル部２１１へ送られる。分離部２０３から分離された番組データも、デスクランブル部２１１へ送られる。デスクランブル部２１１では、復号化されたスクランブル鍵で番組データの復号化を行なう（Ｂ５）。復号化された番組データと番組管理情報４０１を、ディレクトリ管理部２０６へ送る。番組データは、番組蓄積部２０８において、ディレクトリ管理部１０６が指定した蓄積先頭アドレスに蓄積される（Ｂ６）。ＰＩＤの変更時に番組の終了を知り、蓄積を終了する（Ｂ７）。ディレクトリ管理部２０６は、番組管理情報４０１、蓄積先頭アドレス、番組データのサイズから、ディレクトリ情報１５０１を生成する（Ｂ８）。そしてディレクトリ管理部２０６は、ディレクトリ情報１５０１とディレクトリスクランブル鍵１４０４を、ディレクトリ情報暗号部２２２へ送る。ディレクトリ情報暗号部２２２は、ディレクトリスクランブル鍵を使ってディレクトリ情報１５０１の蓄積先頭アドレス１５０３、蓄積サイズ１５０４を暗号化する（Ｂ９）。一部暗号化したディレクトリ情報を、暗号化したディレクトリスクランブル鍵のＫｄ ＩＤを付加して、暗号化ディレクトリ情報１６０１としてディレクトリ情報蓄積部２０７に蓄積する（Ｂ１０）。また、ディレクトリスクランブル鍵を、Ｋｄ暗号部２２１へ送り、暗号化する（Ｂ１１）。暗号化されたディレクトリスクランブル鍵を、ディレクトリスクランブル鍵管理情報１７０１としてＫｄ蓄積部２０９に蓄積する（Ｂ１２）。この時、ディレクトリ情報の蓄積先頭アドレス１６０４と蓄積サイズ１６０５、そしてそれを復号化するディレクトリスクランブル鍵は暗号化されているので、番組の秘匿性を保つことができる。

【００３５】蓄積された番組の視聴の一例を示す。まず、ディレクトリ管理部２０６は、ディレクトリ情報蓄積部２０７に保存されている暗号化ディレクトリ情報１６０１から、必要な情報をシステム制御部２０４に送り出す。システム制御部２０４では、それら情報から、蓄積番組の一覧表画面９０１を作成する。蓄積番組一覧表画面９０１は、シグナルデコード部２１２を通して、表示装置２１４に表示される。ユーザは、その一覧から視聴したい番組を、入力装置２１５によって選択し、決定する。番組を決定すると、その蓄積管理ＩＤ１６０３を、ディレクトリ管理部２０６に送る。ディレクトリ管理部２０６は、ディレクトリ情報蓄積部２０７から、その蓄積管理ＩＤ１６０３を持つ暗号化ディレクトリ情報１６０１を取り出す。そのディレクトリ情報の中のＫｄ ＩＤ１６０２を、Ｋｄ蓄積部２０９へ送り出し、Ｋｄ蓄積部２１７の中から、Ｋｄ ＩＤ１４０２と一致するディレクトリスクランブル鍵１４０４を取り出す。そのディレクトリスクランブル鍵は、Ｋｄ復号部２２０において、復号化される。復号化されたＫｄとその暗号化ディレクトリ情報１６０１を、ディレクトリ情報復号部２２３に送る。ディレクトリ情報復号部２２３は、復号化されたＫｄを使って暗号化ディレクトリ情報１６０１中の暗号化蓄積先頭アドレス１６０４と暗号化蓄積サイズ１６０５を復号化する。ディレクトリ情報の中の先頭アドレス１６０４から、番組蓄積部２０８のそのアドレスに蓄積されている番組データを取り出し、シグナルデコード部２１２へ送る。番組データを、シグナルデコード部２１２において、表示装置２１４に表示できる形式にデコードし、最終的に表示装置２１４に表示し、視聴できるようになる。番組は、番組蓄積部２０８から蓄積サイズ１６０５分のデータを取り出した時点で終了する。

【００３６】次に、ディレクトリスクランブル鍵更新の動作を説明する。ディレクトリスクランブル鍵を配信するとき、ディレクトリスクランブル鍵情報１４０１として配信し、Ｋｄ蓄積部２０９に保存する。放送システムからのディレクトリスクランブル鍵更新要求は、新しいディレクトリスクランブル鍵の配信によって行われる。新しいディレクトリスクランブル鍵情報１４０１を配信するとき、Ｋｄ ＩＤを変更している。受信端末のシステム制御部（ディレクトリスクランブル鍵更新手段）２０４は、常にＫｄ蓄積部２０９に蓄積しているディレクトリスクランブル鍵情報のＫｄ ＩＤ １４０２と、受信した鍵情報のＫｄ ＩＤ １４０２とを比較している。Ｋｄ蓄積部２０９に保存しているＫｄ ＩＤ １４０２と異なるＫｄＩＤを受信したとき、ディレクトリスクランブル鍵の更新を行なう。Ｋｄ蓄積部２０９がディレクトリスクランブル鍵を１つしか保存しない場合の一例を図１９を用いて示す。ディレクトリスクランブル鍵を更新した場合、新しいディレクトリスクランブル鍵情報を放送する。システム制御部２０４は、Ｋｄ蓄積部２０９に蓄積されているディレクトリスクランブル鍵情報のＫｄ ＩＤ１４０２と、受信されたディレクトリスクランブル鍵情報のＫｄ ＩＤ １４０２の比較を常に行なっている。蓄積されているＫｄ ＩＤ １４０２と受信されたＫｄＩＤ １４０２が異なる場合、ディレクトリスクランブル鍵の更新を受け付ける（１７０２）。Ｋｄ蓄積部２０９に蓄積されているディレクトリスクランブル鍵情報を削除する（１７０３）。受信されたディレクトリスクランブル鍵情報１４０１を、Ｋｄ蓄積部２０９に蓄積する（１７０４）。

【００３７】さらに本発明によれば、請求項１２のように、ディレクトリスクランブル鍵を追加蓄積する場合がある。その場合の一例を、図２０を用いて示す。ディレクトリスクランブル鍵が更新された場合、新しいディレクトリスクランブル鍵情報１４０１が放送される。システム制御部２０４では、Ｋｄ蓄積部２０９に蓄積されているディレクトリスクランブル鍵管理情報１７０１のＫｄ ＩＤ １７０２と、受信されたディレクトリスクランブル鍵のＫｄ ＩＤ１４０２の比較を常に行なっている。受信されたディレクトリスクランブル鍵のＫｄ ＩＤ１４０２が、蓄積されているディレクトリスクランブ

ル鍵のＫｄ　ＩＤ　１７０２のいずれも一致しなかった場合、Ｋｄ更新を受け付ける（１８０２）。そして、Ｋｄ蓄積部２０９に空領域があるかないかを調べる（１８０３）。Ｋｄ蓄積部２０９に空領域がある場合、その空領域に受信されたディレクトリスクランブル鍵情報１４０１を保存する（１８０６）。ディレクトリスクランブル鍵管理情報に空領域がない場合、配信日が最も古いディレクトリスクランブル鍵情報を検索する（１８０４）。もっとも古いディレクトリスクランブル鍵情報を削除する（１８０５）。削除された空領域に、新しく受信されたディレクトリスクランブル鍵情報を保存する（１８０６）。

【００３８】ディレクトリスクランブル鍵を更新したときに、更新前のＫｄで暗号化されたディレクトリ情報１６０１を復号化して蓄積し、ディレクトリスクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合、Ｋｄ蓄積部２０９は、ディレクトリスクランブル鍵を1つしか保存しない。ディレクトリスクランブル鍵を更新すると、システム制御部２０４は、更新前の暗号化ディレクトリ情報１６０１をＫｄ蓄積部１０９から取り出す。その中のＫｄ　ＩＤ　１６０２を取り出し、ディレクトリ管理部２０６に送る。ディレクトリ管理部２０６の中から、更新前のＫｄ　ＩＤ　１６０２と一致する暗号化ディレクトリ情報１６０１を取り出し、ディレクトリ情報復号部２２３へ送る。また、更新前のディレクトリスクランブル鍵１４０４をＫｄ復号部２２０へ送る。そこで、ディレクトリスクランブル鍵１４０４を復号し、ディレクトリ情報復号部２２３へ送る。ディレクトリ情報復号部２２３は、そのディレクトリスクランブル鍵１４０４を使って暗号化ディレクトリ情報１６０１の暗号化ディレクトリ情報１６０４を復号する。そして、ディレクトリ管理部２０６は、暗号化ディレクトリ情報のＫｄ　ＩＤ１６０２に何も指定せず、暗号化蓄積先頭アドレス１６０４に復号化された蓄積先頭アドレスを書き込み、暗号化蓄積サイズ１６０５に復号化された蓄積サイズを書き込む。新たに生成された暗号化ディレクトリ情報を、ディレクトリ情報蓄積部２０７に保存する。

【００３９】このように蓄積された番組を視聴する場合は次のようになる。視聴者が視聴要求したとき、その暗号化ディレクトリ情報のＫｄ　ＩＤ　１６０２に何も指定がなかった場合、そのディレクトリ情報のディレクトリ情報をそのまま参照し、番組データを番組蓄積部２０８から取り出す。番組データを、シグナルデコード部２１２に送り、表示装置２１４に表示できる形式変換し、表示装置２１４に表示する。

【００４０】ディレクトリスクランブル鍵を更新したときに、更新前のディレクトリスクランブル鍵を複数個蓄積し、ディレクトリスクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。ディレクトリスクランブル鍵を更新する場合、新しいディレクトリスクランブル鍵情報１４０１を放送する。システム制御部２０４では、Ｋｄ蓄積部２０９に蓄積されているディレクトリスクランブル鍵情報のＫｄ　ＩＤ　１４０２と、受信されたディレクトリスクランブル鍵情報のＫｄＩＤ　１４０２の比較を常に行なっている。受信されたディレクトリスクランブル鍵のＫｄ　ＩＤ１４０２が、蓄積されているディレクトリスクランブル鍵のＫｄＩＤ１４０２のいずれとも一致しなかった場合、Ｋｄ蓄積部２０９の空領域に、受信されたディレクトリスクランブル鍵情報１４０１を蓄積する。Ｋｄ蓄積部２０９に空領域がない場合、配信日が最も古いディレクトリスクランブル鍵情報１４０１を取り出し、システム制御部２０４へ送り、削除する。システム制御部２０４は、そのディレクトリスクランブル鍵情報１４０１をディレクトリ管理部２０６に送る。ディレクトリ管理部２０６は、ディレクトリ情報蓄積部２０７にあるＫｄ　ＩＤと一致する暗号化ディレクトリ情報１６０１を取り出し、ディレクトリスクランブル鍵１４０４と共にディレクトリ情報復号部へ送り、復号化する。復号化された蓄積先頭アドレス１６０４と蓄積サイズ１６０５から、番組蓄積部のその蓄積先頭アドレスに蓄積されている番組データを消去する。そして、ディレクトリスクランブル鍵を消去する。また、Ｋｄ蓄積部２０９の空領域に、新しいディレクトリスクランブル鍵情報を保存する。

【００４１】次にディレクトリスクランブル鍵を更新したときに、更新前のＫｄで暗号化されたディレクトリ情報１６０１を復号化し、新しいディレクトリスクランブル鍵で再暗号化して蓄積し、ディレクトリスクランブル鍵の更新前の番組を視聴可能にする場合の動作を説明する。この場合にも、Ｋｄ蓄積部１０９は、ディレクトリスクランブル鍵を1つしか保存しない。ディレクトリスクランブル鍵を更新する。

【００４２】場合、システム制御部２０４は、Ｋｄ蓄積部２０９から更新前のディレクトリスクランブル鍵を取り出し、Ｋｄ復号部２０９へ送る。Ｋｄ復号部でディレクトリスクランブル鍵を復号し、ディレクトリ情報復号部２２３へ送る。ディレクトリ情報復号部２２３は、ディレクトリ情報蓄積部２０７から、暗号化ディレクトリ情報１６０１を取り出し、その中の暗号化蓄積先頭アドレス１６０４と暗号化蓄積サイズ１６０５をディレクトリスクランブル鍵１４０４を使って復号する。また、更新された新しいディレクトリスクランブル鍵もＫｄ復号部２２０において復号化し、ディレクトリ情報暗号部２２２に送る。先程復号化された蓄積先頭アドレス１６０４と蓄積サイズ１６０５を、ディレクトリ情報暗号部２２２へ送り、新しい鍵によって暗号化する。ディレクトリ管理部２０６において、再暗号化された蓄積先頭アドレス１６０４と蓄積サイズ１６０５から、暗号化ディレクトリ情報１６０１を再構成する。この時、Ｋｄ　ＩＤ

１６０２には、暗号化を行なった新しいディレクトリスクランブル鍵のＫｄ　ＩＤを指定する。暗号化ディレクトリ情報１６０１を、ディレクトリ情報蓄積部２０７に蓄積する。

【００４３】次に、ディレクトリ情報から蓄積番組用の番組一覧を作成する方法の動作を説明する。まず、ディレクトリ管理部２０６は、ディレクトリ情報蓄積部２０７に保存されている暗号化蓄積管理情報１６０１の蓄積管理ＩＤ　１６０２、番組管理情報４０１の中に記述されているチャンネル４０３、日時４０４、タイトル４０８、課金情報４０５、番組情報４０９を取り出し、システム制御部２０４へ送る。これらの情報から、蓄積番組表示情報１１０１を生成する。蓄積番組表時情報１１０１の日時１１０４から、蓄積番組一覧画面９０１の日付、開始時間、終了時間を作り、蓄積番組表時情報のチャンネル１１０３から蓄積番組一覧画面のチャンネルを作り、蓄積番組表時情報のタイトル１１０８から、蓄積番組一覧画面のタイトルを生成し、蓄積番組一覧画面９０１を表示装置２１４に表示する。

【００４４】以上より、ディレクトリスクランブル鍵を暗号化すれば、これは蓄積された番組データのアドレス管理を行っているため、蓄積された番組おのおのを暗号化せずにすむので、スクランブル処理がより早くなる。

【００４５】

【発明の効果】本発明によれば、有料放送の番組を蓄積する場合に、暗号化されて放送された番組をそのまま蓄積し、その暗号を解くためのスクランブル鍵を暗号化して蓄積することにより、蓄積された番組の秘匿性を保護することが出来、蓄積された番組の視聴時に課金を行うことが出来る。番組の暗号化を行うスクランブル鍵を解読され、番組の秘匿性を破られた場合に、スクランブル鍵を新たに更新することによって、番組の秘匿性を回復することが出来る。

【００４６】また、番組を蓄積する場合に、番組を復号化して蓄積するが、そのディレクトリ情報をその情報を暗号化するためのディレクトリスクランブル鍵で暗号化することによって、蓄積された番組の読み込みを不可能にし、番組の秘匿性を保護することが出来る。また、ディレクトリスクランブル鍵を放送波にのせて更新することによって、ディレクトリスクランブル鍵を破られた場合の対処を行うことが出来る。また、番組のジャンル毎にディレクトリスクランブル鍵を変更して暗号化を行うことによって、蓄積された番組をジャンル毎に管理することが出来る。

【図面の簡単な説明】

【図１】本発明における番組を蓄積する際、暗号化した番組を蓄積し、視聴する際に番組の復号化を行なう蓄積型受信装置の内部構成を示すブロック図

【図２】番組の暗号化を行なうスクランブル鍵が配信されるときの状態であるスクランブル鍵情報のフレーム図

【図３】番組を管理する情報である番組管理情報のフレーム図

【図４】放送波によって配信されるＥＰＧ情報である番組プログラム管理情報を示す説明図

【図５】番組の蓄積の予約を管理する予約管理情報のフレーム図

【図６】蓄積番組を管理するディレクトリ情報のフレーム図

【図７】番組を予約するための番組一覧画面を示す説明図

【図８】蓄積された番組を選択するための蓄積番組一覧表画面を示す説明図

【図９】図１の受信装置における、番組の蓄積動作を示すフロー図

【図１０】課金管理部によって管理されている課金管理情報を示す説明図

【図１１】蓄積番組用の番組一覧を表示するためにシステム制御部において生成される蓄積番組表時情報を示す説明図

【図１２】図１の受信装置における、スクランブル鍵を１つしか保存しない場合のスクランブル鍵の更新の動作を示すフロー図

【図１３】図１の受信装置における、スクランブル鍵を複数保存する場合のスクランブル鍵更新の動作を示すフロー図

【図１４】本発明の番組を蓄積する際、ディレクトリ情報を暗号化して番組を蓄積する積型受信装置の内部構成を示すブロック図

【図１５】放送波によってディレクトリスクランブル鍵が配信されるときの状態であるディレクトリスクランブル鍵情報のフレーム図

【図１６】ディレクトリ管理部によって生成される暗号化される前のディレクトリ情報のフレーム図

【図１７】ディレクトリ情報蓄積部に蓄積される、暗号化された後のディレクトリ情報のフレーム図

【図１８】図１４の受信装置おける、ディレクトリ情報を暗号化して番組を蓄積する場合のフロー図

【図１９】図２の受信装置における、番組の蓄積動作を示すフロー図

【図２０】図２の受信装置における、ディレクトリスクランブル鍵を１つしか保存しない場合のディレクトリスクランブル鍵更新の動作を示すフロー図

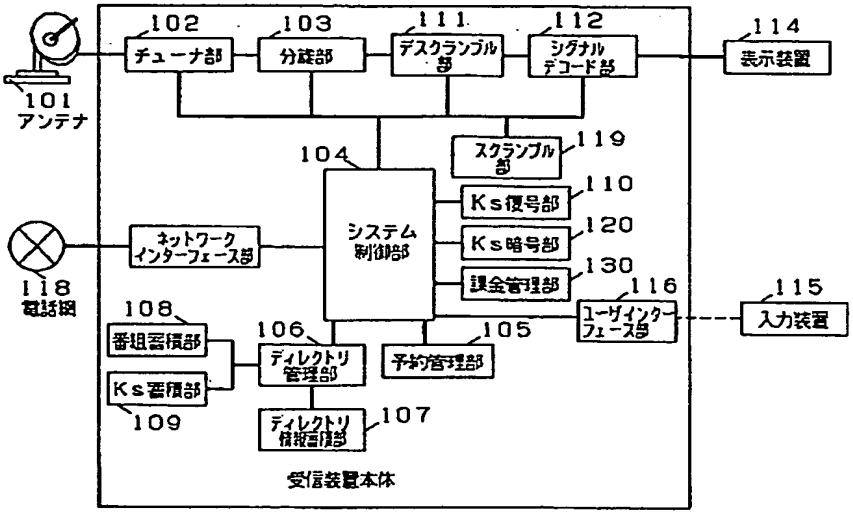
【図２１】図２の受信装置における、ディレクトリスクランブル鍵を複数保存する場合のディレクトリスクランブル鍵更新の動作を示すフロー図

【符号の説明】

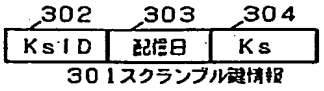
１０４　システム制御部
１０８　番組蓄積部
１０９　Ｋｓ蓄積部（スクランブル鍵蓄積部）
２０４　システム制御部

２０６　ディレクトリ管理部
２０８　番組蓄積部
２２２　ディレクトリ情報暗号部

【図１】

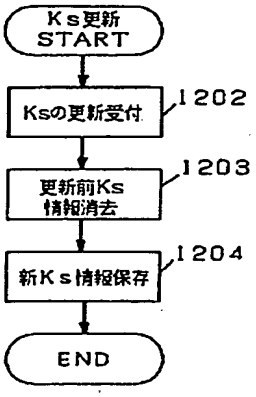


【図２】



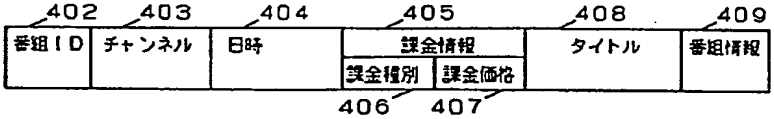
３０１スクランブル鍵情報

【図１２】



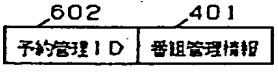
1201

【図３】



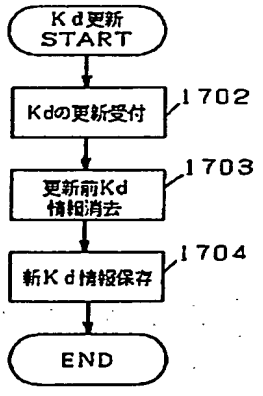
401　番組管理情報

【図５】



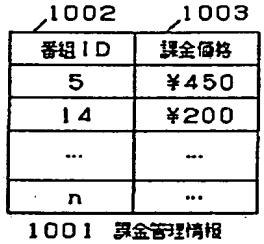
601　予約管理情報

【図１９】



1701

【図１０】



1002 番組ID	1003 課金価格
5	¥450
14	¥200
…	…
n	…

1001　課金管理情報

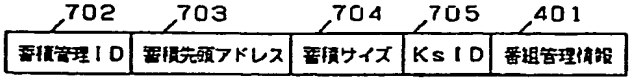
【図４】

401

番組ID	チャンネル	日時	課金情報		タイトル	番組情報
			課金種別	課金価格		
0	Channel 1	10/24 19:00-20:00	蓄積時	¥300	ニュース	…
1	Channel 2	10/24 19:00-19:30		¥0	ニュース	…
…	…	…	…	…	…	…
n	Channel 1	10/24 21:00-23:00	視聴時	¥400	映画「東京物語２」	…

501 番組プログラム管理情報

【図６】



701 ディレクトリ情報

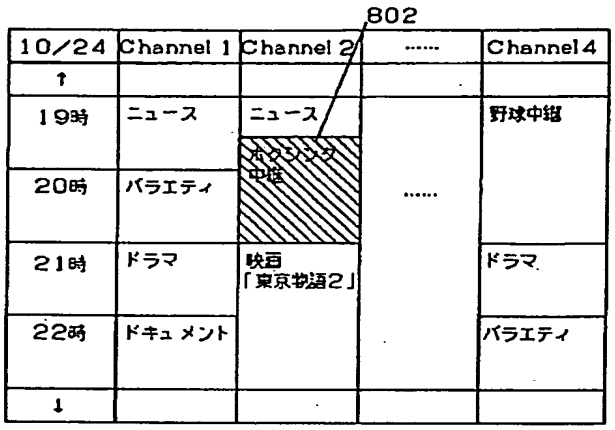
【図８】

番号	日付	開始時間	終了時間	チャンネル	タイトル
1	10/16	21:00	23:00	Channel 5	映画「ここより過去に」
2	10/24	19:30	21:00	Channel 7	ネタバレ番組
…	…	…	…	…	…
n	10/30	15:00	16:00	Channel 7	芸能情報番組

902

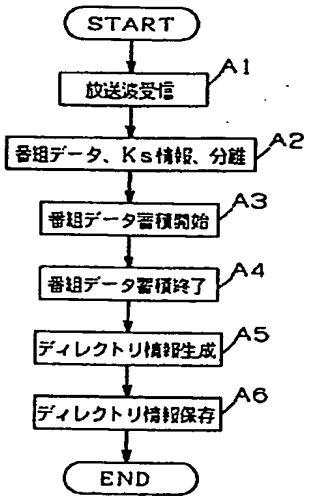
901 蓄積番組一覧表画面

【図７】

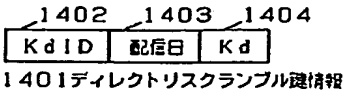


801 番組一覧画面

【図９】

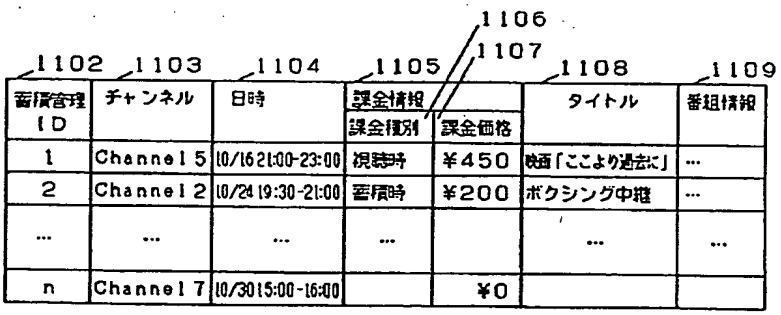


【図１５】



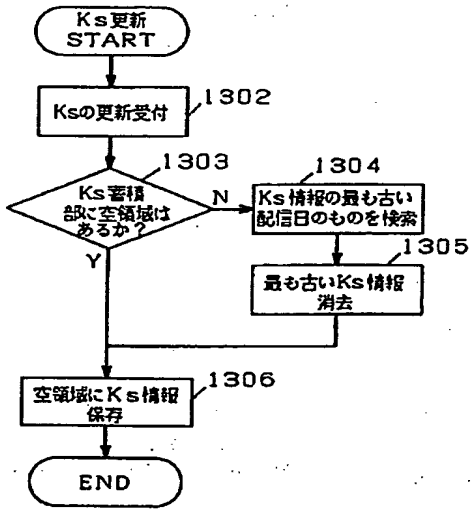
1401ディレクトリスクランブル鍵情報

【図１１】



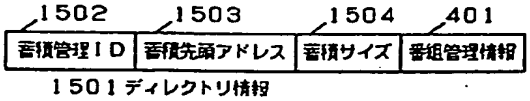
1101 蓄積番組表示情報

【図１３】



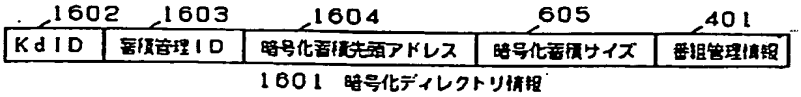
1301

【図１６】



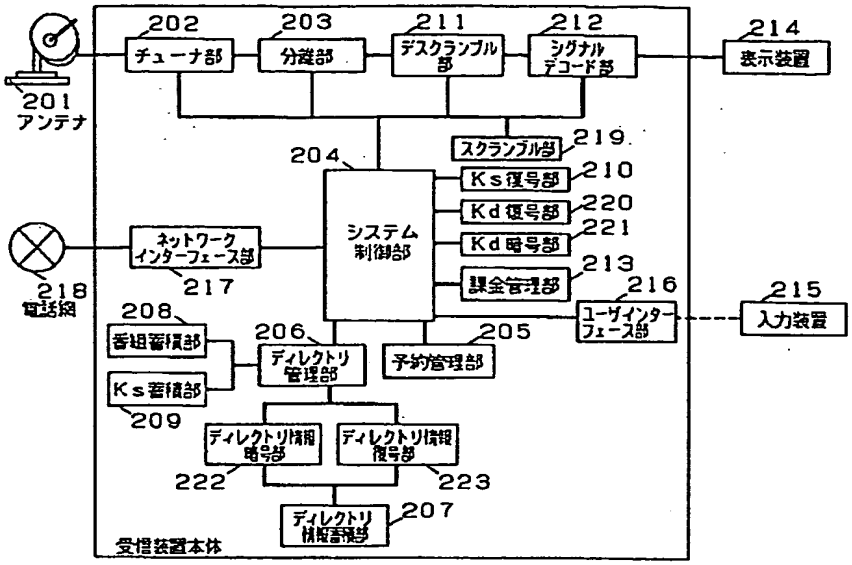
1501 ディレクトリ情報

【図１７】

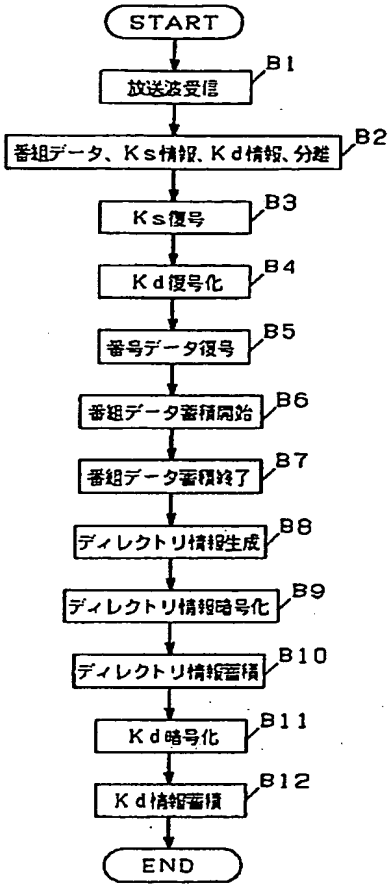


1601 暗号化ディレクトリ情報

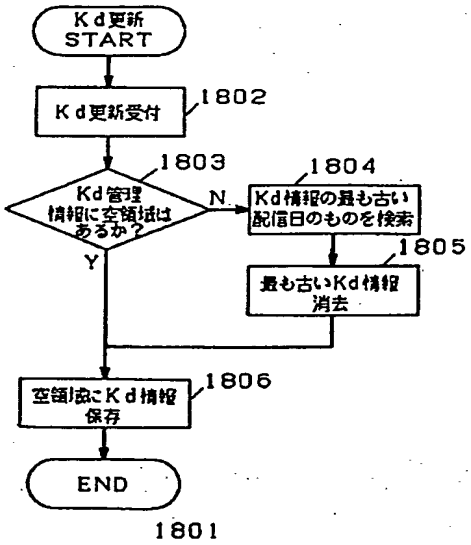
【図１４】



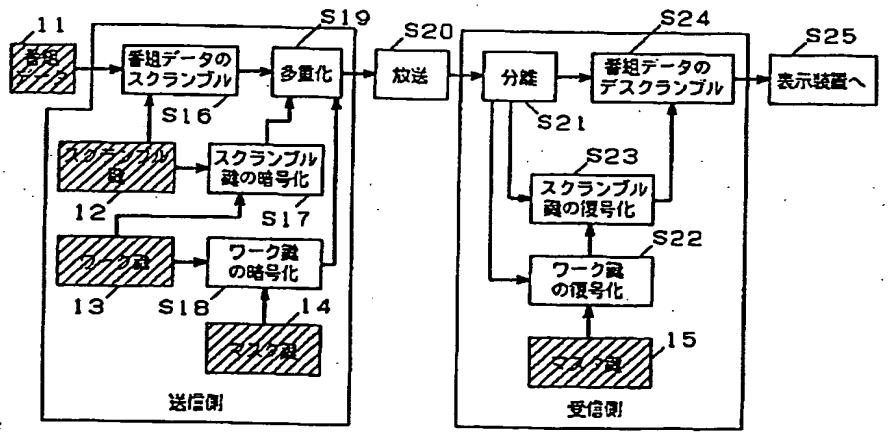
【図１８】



【図２０】



【図２１】



フロントページの続き

(72)発明者　町田　和弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　片岡　充照
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　中村　康浩
大阪府門真市大字門真1006番地　松下電器
産業株式会社内